(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－288939

(43)公開日　平成８年(1996)11月１日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｌ	9/06			Ｈ０４Ｌ	9/02	Ｚ	
	9/14		7259－5Ｊ	Ｇ０９Ｃ	1/00		
Ｇ０９Ｃ	1/00			Ｈ０４Ｈ	1/02	Ｅ	
Ｈ０４Ｈ	1/02					Ｆ	
				Ｈ０４Ｎ	7/167	Ｚ	

審査請求　未請求　請求項の数２　ＯＬ　（全８頁）　最終頁に続く

(21)出願番号　特願平7－90641

(22)出願日　平成７年(1995)４月17日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　▲高▼野　裕昭
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

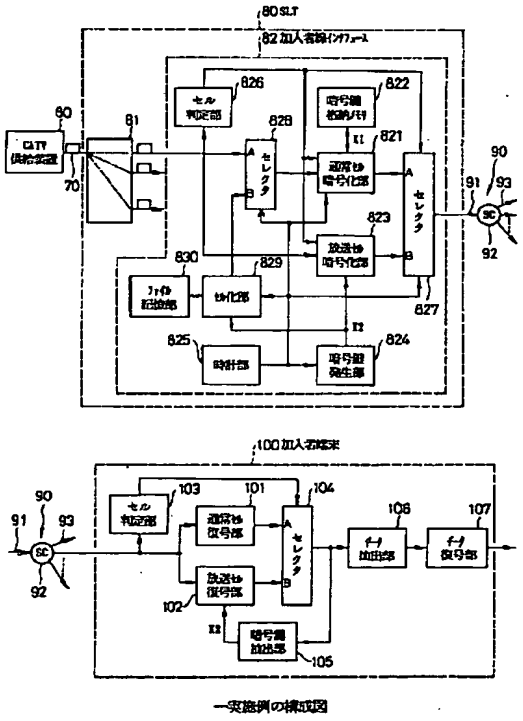
(74)代理人　弁理士　工藤　宣幸

(54)【発明の名称】　放送システム

(57)【要約】

【目的】　時間的な放送スイッチを用いることなく、各加入者線に接続された複数の契約端末にのみ放送サービスを提供することができるようにする。

【構成】　回線終端装置８０の放送セル暗号化部８２３と、暗号鍵発生部８２４と、時計部８２４等は、所定の周期で更新される暗号鍵Ｋ２を使って、放送セルを暗号化する機能を有する。セル化部８２９と、ファイル記憶部８３０と、通常セル暗号化部７２１等は、暗号鍵Ｋ２が更新されるたびに、この暗号鍵Ｋ２をセル化し、このセルを各契約者に予め付与された暗号鍵Ｋ１で暗号化する機能を有する。加入者端末１００の通常セル復号部１０１は、予め自端末に付与された暗号鍵Ｋ１を使って受信セルを復号する機能を有する。暗号鍵抽出部１０５はこの復号出力から暗号鍵Ｋ２を抽出する機能を有する。放送セル復号部１０２は、この抽出出力を使って受信セルを復号する機能を有する。



一実施例の構成図

1

【特許請求の範囲】

【請求項１】　放送情報の送信側に設けられ、この放送情報の送信信号を第１の暗号鍵を使って暗号化する第１の暗号化手段と、

前記放送情報の送信側に設けられ、前記第１の暗号鍵を所定の周期で更新する暗号鍵更新手段と、

前記第１の暗号鍵が更新されるたびに、この第１の暗号鍵の送信信号を各契約者ごとに予め付与された第２の暗号鍵を使って暗号化する第２の暗号化手段と、

前記放送情報の受信側に設けられ、受信信号を予め自分に付与された前記第２の暗号鍵を使って復号する第１の復号手段と、

前記放送情報の受信側に設けられ、前記第１の復号手段の復号出力から前記第１の暗号鍵を抽出する暗号鍵抽出手段と、

前記放送情報の受信側に設けられ、前記暗号鍵抽出手段の抽出出力を使って前記受信信号を復号する第２の復号手段とを具備したことを特徴とする放送システム。

【請求項２】　前記第１の暗号化手段と、前記暗号鍵更新手段と、前記第２の暗号化手段は、加入者網の加入者線終端装置に設けられ、

前記第１の復号手段と、前記暗号鍵抽出手段と、前記第２の復号手段は、加入者線を介して前記加入者線終端装置に接続される加入者端末に設けられていることを特徴とする請求項１記載の放送システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、伝送路として、例えば、広帯域サービス総合ディジタル網（以下「Ｂ－ＩＳＤＮ」という。）を使って放送を行う放送システムに関する。

【０００２】

【従来の技術】近年、電気通信の分野においては、電話網のような加入者網として、Ｂ－ＩＳＤＮの導入が進められている。このＢ－ＩＳＤＮにおいては、通信サービスとして、有線テレビジョン（以下「ＣＡＴＶ」という。）をはじめとする放送型サービスの提供が予想される。このため、例えば、下記の文献等に記載されるように、Ｂ－ＩＳＤＮにおける放送型サービスの提供に関する研究開発が盛んに行われている。

【０００３】文献：「マルチメディアサービスを提供する広帯域アクセス系の検討」

信学技報　TECHNICAL REPORT OF IEICE. CS94-18. OSC94-8(1994-05)

図２は、Ｂ－ＩＳＤＮを使ったＣＡＴＶシステムの構成の一例を示すブロック図である。

【０００４】図示のＣＡＴＶシステムにおいては、ＣＡＴＶ供給装置１０から出力されたＣＡＴＶ信号の放送セルは、Ｂ－ＩＳＤＮの中核をなす長距離網２０を介して加入者線終端装置（ＳＬＴ）３０に供給される。

2

【０００５】加入者線終端装置３０に供給された放送セルは、複数の加入者線４０に振り分けられる。各加入者線４０に振り分けられた放送セルは、この加入者線４０に接続された複数の加入者端末（ＯＮＵ）５０に振り分けられる。

【０００６】各加入者線４０は、例えば、パッシブダブルスター方式の伝送路によって構成されている。すなわち、各加入者線４０は、加入者線終端装置３０に接続される１本の光ファイバ４１と、スターカプラ（ＳＣ）４２と、各加入者端末５０に接続される複数の光ファイバ４３によって構成されている。

【０００７】しかしながら、加入者線４０をパッシブダブルスター方式の伝送路で形成するような構成では、放送サービスの契約者以外の者にも放送サービスが提供されてしまうという問題が生じる。

【０００８】すなわち、放送サービスの契約は、通常、放送チャネルごとに行われる。また、Ｂ－ＩＳＤＮを使った放送サービスの場合、さらに、時間単位の契約が考えられる。言い換えれば、番組単位の契約が考えらる。

【０００９】このような契約環境の下では、各加入者線４０に接続された複数の加入者端末５０がすべて契約者の加入者端末（以下「契約端末」という。）とは限らない。したがって、加入者線４０をパッシブダブルスター方式の伝送路で形成するような構成では、放送サービスの契約者以外の者にも放送サービスが提供されてしまうという問題が生じる。

【００１０】この問題に対処するために、従来は、加入者線終端装置３０において、予め各加入者端末５０に付与された暗号鍵を使って、各契約者ごとに放送セルを暗号化して送信するようになっていた。

【００１１】このような構成によれば、各契約端末５０しか受信セルを復号することができないので、契約者にのみ放送サービスを提供することができる。

【００１２】

【発明が解決しようとする課題】しかしながら、このような構成では、放送セルの放送スイッチとして、空間的な放送スイッチのほかに、時間的な放送スイッチが必要になるという問題があった。

【００１３】ここで、空間的な放送スイッチ３１とは、図３に示すように、ＣＡＴＶ供給装置１０から供給される放送セルを複数の出線３２に振り分けるスイッチである。

【００１４】また、時間的な放送スイッチ３３とは、図４に示すように、放送セルを契約端末数分だけ複写し、各複写セルを各出線３２に時分割で出力することにより、１つの加入者線４０に接続されている複数の契約端末５０に放送セルを振り分けるスイッチである。

【００１５】このような時間的な放送スイッチが必要になると、各加入者の使用可能な帯域が狭められてしまうという問題が生じる。

【００１６】また、図５に示すように、放送スイッチ３３の内部に放送セルの複写部３４を設ける構成では、放送セルを最大で［出線数］＊［出線に接続される加入者端末数］分複写しなければならないため、バッファメモリの負荷が大きくなってしまうという問題が生じる。

【００１７】さらに、図６に示すように、放送スイッチ３３の出線３２上に放送セルの複写部３４を設けるような構成では、各出線３２ごとにバッファメモリを設けなければならないという問題が生じる。

【００１８】したがって、加入者線４０として、パッシブダブルスター方式の伝送路を用いる放送システムにおいては、時間的な放送スイッチ３３を用いることなく、放送を行うことができるような技術が望まれる。

【００１９】

【課題を解決するための手段】上記課題を解決するために、この発明は、放送情報の送信信号を所定の周期で更新される第１の暗号鍵を使って暗号化して送信し、かつ、この第１の暗号鍵が更新されるたびに、この第１の暗号鍵の送信信号を各契約者ごとに予め付与された第２の暗号鍵を使って暗号化して送信するようにしたものである。

【００２０】

【作用】上記構成においては、放送情報の送信側では、放送情報の送信信号を第１の暗号鍵で暗号化して送信する処理が実行される。また、第１の暗号鍵が更新されるたびに、この暗号鍵の送信信号を各契約者に予め付与された第２の暗号鍵で暗号化して送信する処理が実行される。

【００２１】一方、放送情報の受信側では、予め自分に付与された第２の暗号鍵を使って受信信号を復号する処理が実行される。また、この復号出力から第１の暗号鍵を抽出する処理が実行される。さらに、この抽出出力を使って受信信号を復号する処理が実行される。

【００２２】このような構成によれば、受信された第１の暗号鍵の送信信号が予め自分に付与された第２の暗号鍵で暗号化されたものであれば、この受信信号から正確に第１の暗号鍵を抽出することができる。これにより、時間的な放送スイッチを用いることなく、受信された放送情報の送信信号を正確に復号することができる。

【００２３】

【実施例】以下、図面を参照しながら、この発明の実施例を詳細に説明する。

【００２４】図１は、この発明の一実施例の構成を示すブロック図である。

【００２５】なお、図１は、この発明を、Ｂ－ＩＳＤＮを使ったＣＡＴＶシステムに適用した場合を代表として示す。また、図１は、この発明を、放送セルのほかに通常セルの伝送機能を有するシステムに適用した場合を代表として示す。ここで、通常セルとは、１つの加入者端末１００にのみ供給されるＡＴＭ（非同期転送モード）セルである。

【００２６】図示の放送システムは、ＣＡＴＶ供給装置６０と、長距離網７０と、加入者線終端装置８０と、複数の加入者線９０と、複数の加入者端末１００を有する。なお、図には、１つの加入者線９０と、１つの加入者端末１００を示す。

【００２７】ここで、ＣＡＴＶ供給装置60_iは、ＣＡＴＶ信号の放送セルを出力する機能を有する。長距離網７０は、ＡＴＭセル（放送セルや通常セル）を加入者線終端装置８０まで伝送する機能を有する。加入者線終端装置８０は、加入者線９０を終端する機能を有する。加入者線９０は、加入者端末１００と加入者線終端装置８０とを接続する機能を有する。加入者端末１００は、ＣＡＴＶ信号のＡＴＭセルを受信する機能を有する。

【００２８】加入者線終端装置８０は、放送スイッチ８１と、複数の加入者線インタフェース８２を有する。

【００２９】ここで、放送スイッチ８１は、長距離網７０を介して送られてきたＡＴＭセルを複数の加入者線インタフェース８２に分配する機能を有する。図には、１つの加入者線インタフェース８２を示す。各加入者線インタフェース８２は、放送スイッチ８１と加入者線９０とを接続する機能を有する。

【００３０】各加入者線９０は、１つの光ファイバ９１と、１つのスターカプラ９２と、複数の光ファイバ９３からなるパッシブダブルスター方式の伝送路として構成されている。

【００３１】ここで、光ファイバ９１は、対応する加入者線インタフェース８０とスターカプラ９２とを接続する機能を有する。光カプラ９２は、光ファイバ９１から供給されるＡＴＭセルを分岐する機能を有する。光ファイバ９３は、スターカプラ９２と各加入者端末１００とを接続する機能を有する。

【００３２】加入者線インタフェース８２は、通常セル暗号化部８２１と、暗号鍵格納メモリ８２２と、放送セル暗号化部８２３と、暗号鍵発生部８２４と、時計部８２５と、セル判定部８２６と、セレクタ８２７，８２８と、セル化部８２９と、ファイル記憶部８３０を有する。

【００３３】ここで、通常セル暗号化部８２１は、通常セルの宛先の加入者端末１００に予め付与された暗号鍵Ｋ１を使って、当該通常セルを暗号化する機能を有する。暗号鍵格納メモリ８２２は、対応する加入者線９０に接続された複数の加入者端末１００のそれぞれに予め付与された暗号鍵Ｋ１を各加入者線１００ごとに保持する機能を有する。

【００３４】放送セル暗号化部８２３は、暗号鍵Ｋ２を使って、放送セルを暗号化する機能を有する。暗号鍵発生部８２４は、暗号鍵Ｋ２を出力する機能を有する。また、この暗号鍵発生部８２４は、時計部８２５から供給される制御信号に基づいて、暗号鍵Ｋ２を所定の周期で

更新する機能を有する。時計部８２５は、暗号鍵Ｋ２の更新タイミングを示す制御信号を出力する機能を有する。

【００３５】セル判定部８２６は、放送スイッチ８１から出力されるＡＴＭセルが通常セルか放送セルかを判定する機能を有する。

【００３６】セレクタ８２７は、セル判定部８２６によりＡＴＭセルが通常セルと判定されると、通常セル暗号化部８２１の出力を選択し、放送セルと判定されると、放送セル暗号化部８２３の出力を選択する機能を有する。また、このセレクタ８２７は、暗号鍵Ｋ２が変更されると、セル判定部８２６の判定結果に関係なく、一時的に、通常セル暗号化部８２１の出力を選択する機能を有する。

【００３７】セレクタ８２８は、通常は、放送スイッチ８１から出力されるＡＴＭセル（放送セルや通常セル）を選択し、暗号鍵Ｋ２が更新されると、一時的に、セル化部８３０から出力される暗号鍵のセルを選択する機能を有する。この選択出力は、通常セル暗号化部８２１に供給される。

【００３８】セル化部８２９は、暗号鍵Ｋ２の更新時に、この暗号鍵Ｋ２をセル化する機能を有する。このセルは通常セルとして形成される。この通常セルを以下暗号鍵セルという。ファイル記憶部８３０は、加入者の情報ファイル（以下「加入者ファイル」という。）を格納する機能を有する。この加入者ファイルには、加入者に関する各種情報が登録される。

【００３９】なお、暗号鍵発生部８２４は、各放送チャネルごとに暗号鍵Ｋ２を発生する。また、放送セル暗号化部８２３は、受け取った放送セルの放送チャネルを判定し、判定した放送チャネルに対応する暗号鍵Ｋ２で当該放送セルを暗号化する。

【００４０】加入者端末１００は、通常セル復号部１０１と、放送セル復号部１０２と、セル判定部１０３と、セレクタ１０４と、暗号鍵抽出部１０５と、データ抽出部１０６と、データ復号部１０７を有する。

【００４１】ここで、通常セル復号部１０１は、対応する光ファイバ９３を介して送られてきた受信セルを予め自装置に付与された暗号鍵Ｋ１を使って復号する機能を有する。同様に、放送セル復号部１０２は、この受信セルを暗号鍵抽出部１０５の抽出出力を使って復号する機能を有する。

【００４２】セル判定部１０３は、受信セルが通常セルか放送セルかを判定する機能を有する。セレクタ１０４は、セル判定部１０３によりセルが通常セルと判定されると、通常セル復号部１０１の出力を選択し、放送セルと判定されると、放送セル復号部１０２の出力を選択する機能を有する。暗号鍵抽出部１０５は、セレクタ１０４の選択出力から暗号鍵Ｋ２を抽出する機能を有する。

【００４３】データ抽出部１０６は、セレクタ１０４の選択出力からＡＴＭセルのペイロード部分に挿入されているデータを抽出する機能を有する。データ復号部１０７は、データ抽出部１０６により抽出されたデータを復号する機能を有する。

【００４４】上記構成において、動作を説明する。

【００４５】まず、放送システム全体の動作を説明する。

【００４６】ＣＡＴＶ供給装置６０から出力された放送セルは、長距離網７０を介して加入者線終端装置８０に供給される。また、この加入者線終端装置８０には、放送セル以外の通常セルも供給される。

【００４７】加入者線端末装置８０は、入力セルが通常セルであれば、これを、その宛先に基づいて、複数の加入者線９０のいずれか１つに送出する。加入者線９０に送出された通常セルは、この加入者線９０に接続された複数の加入者端末１００に供給される。この複数の加入者端末１００に供給された通常セルは、その宛先に応じた加入者端末１００でのみ正常に復号される。

【００４８】これに対し、入力セルが放送セルであれば、これを複数の加入者線９０に振り分ける。各加入者線９０に振り分けられた放送セルは、この加入者線９０に接続された複数の加入者端末１００に供給される。この複数の加入者端末１００に供給された放送セルは、当該放送チャネルの契約端末１００でのみ正常に復号される。以上が、図１の放送システムの全体的な動作である。

【００４９】次に、加入者線終端装置８０の動作を説明する。

【００５０】ＣＡＴＶ供給装置６０から加入者線終端装置８０に送られてきた放送セルは、まず、放送スイッチ８１に供給される。放送スイッチ８１は、入力セルが通常セルであれば、これを複数の加入者線インタフェース８２のうち、その宛て先に応じた加入者線インタフェース８２に供給する。これに対し、放送セルであれば、複数の加入者線インタフェース８２に供給する。

【００５１】この加入者線インタフェース８２の動作は、暗号鍵Ｋ２の更新時以外の期間の動作と暗号鍵Ｋ２の更新時の動作に大別される。したがって、以下の説明では、この２つの場合に分けて、加入者線インタフェース８２の動作を説明する。

【００５２】まず、暗号鍵Ｋ２の更新時以外の期間の動作を説明する。

【００５３】放送スイッチ８１から出力されるＡＴＭセル（通常セルや放送セル）は、セレクタ８２８と、放送セル暗号化部８２３と、セル判定部８２６に供給される。また、セル化部８２９から出力される暗号鍵セルは、セレクタ８２８に供給される。

【００５４】セレクタ８２８は、暗号鍵Ｋ２の更新時以外の期間は、放送スイット８１から出力されるＡＴＭセルを選択する。これにより、この場合は、通常セル暗号

化部８２１には、放送スイッチ８１から出力されるＡＴＭセルが供給される。

【００５５】セル判定部８２６は、入力セルが通常セルか放送セルかを判定する。この判定結果は、通常セル暗号化部８２１と、放送セル暗号化部８２３と、セレクタ８２７に供給される。

【００５６】通常セル暗号化部８２１は、入力セルが通常セルの場合は、この入力セルの宛先の加入者端末１００に予め定められた暗号鍵Ｋ１を使って、この入力セルを暗号化する。この暗号鍵Ｋ１は、暗号鍵格納メモリ８２２から読み出される。これに対し、放送セルの場合は、この暗号化処理を中止する。この通常セル暗号化部８２１の出力は、セレクタ８２７に供給される。

【００５７】放送セル暗号化部８２３は、入力セルが放送セルの場合は、暗号鍵発生部８２４から出力される暗号鍵Ｋ２を使って、この入力セルを暗号化する。これに対し、通常セルの場合は、この暗号化処理を中止する。この放送セル暗号化部８２３の出力は、セレクタ８２７に供給される。

【００５８】セレクタ８２７は、セルが通常セルの場合は、通常セル暗号化部８２１の出力を選択し、放送セルの場合は、放送セル暗号化８２３の出力を選択する。これにより、セルが通常セルの場合は、セレクタ８２７から通常セルの暗号化出力が出力され、放送セルの場合は、放送セルの暗号化出力が出力される。

【００５９】この暗号化出力は、加入者線９０を介してこの加入者線９０に接続されるすべての加入者端末１００に供給される。以上が、暗号鍵Ｋ２の更新時以外の期間の動作である。

【００６０】次に、暗号鍵Ｋ２の更新時の動作を説明する。

【００６１】この場合も、放送スイッチ８１から出力されるＡＴＭセルは、セレクタ８２８と、セル判定部８２６と、放送セル暗号化部８２３に供給される。また、セル化部８２９から出力される暗号鍵セルは、セレクタ８２８に供給される。さらに、セル判定部８２６の判定結果は、通常セル暗号化部８２１と、放送セル暗号化部８２３と、セレクタ８２７に供給される。

【００６２】しかし、この場合、セレクタ８２８では、時計部８２５から出力される制御信号に従って、セル化部８２９の出力が選択される。また、通常セル暗号化部８２１では、セル判定部８２６の判定結果に関係なく、通常セル入力時の動作が行われる。さらに、セレクタ８２７では、セル判定部８２６の判定結果に関係なく、通常セル暗号化部８２１の出力が選択される。

【００６３】これにより、この場合は、セル化部８２８から出力される暗号鍵セルがセレクタ８２８を介して通常セル暗号化部８２１に供給され、暗号化される。この暗号化出力は、セレクタ８２７を介して加入者線９０に出力され、この加入者線９０に接続された複数の加入者端末１００に供給される。以上が暗号鍵Ｋ２の更新時の動作である。

【００６４】ここで、セル化部８２９の動作を詳細に説明する。

【００６５】このセル化部８２９では、暗号鍵Ｋ２の更新時、まず、暗号鍵発生部８２４から出力されるある放送チャネルの暗号鍵Ｋ２をセル化する処理が実行される。これにより、暗号鍵セルが得られる。この暗号鍵セルは、通常セルとして形成される。但し、この段階では、その宛先情報（仮想パス識別子や仮想チャネル識別子等）は挿入されていない。

【００６６】次に、この暗号鍵セルを複写する処理が実行される。この複写は、当該放送チャネルの契約者数分だけ繰り返される。但し、この場合の契約者数は、対応する加入者線９０に接続されている契約者数である。

【００６７】このとき、同時に、各契約者の宛先情報を挿入する処理も実行される。この宛先情報は、ファイル記憶部８３０に格納されている加入者ファイルから読み出される。

【００６８】このようにして生成された契約者数分の暗号鍵セルは、順次セレクタ８２８を介して、通常セル暗号化部８２１に供給される。この後、次の放送チャネルの暗号鍵Ｋ２について、上述したような処理が実行される。以下、同様に、すべての放送チャネルの暗号鍵Ｋ２について、上述した処理が繰り返される。

【００６９】通常セル暗号化部８２１に供給された暗号鍵セルは、放送スイッチ８１から供給される通常セルと同様に、その宛先に対応する暗号鍵Ｋ１を使って暗号化される。以上がセル化部８２９の動作である。

【００７０】次に、加入者端末１００の動作を説明する。

【００７１】光ファイバ９３を介して送られてきた受信セル（通常セル（暗号鍵セルを含む）や放送セル）は、通常セル復号部１０１と、放送セル復号部１０２と、セル判定部１０３に供給される。

【００７２】通常セル復号部１０１に供給された受信セルは、当該端末に割り当てられた暗号鍵Ｋ１を使って復号される。この復号出力は、セレクタ１０４に供給される。また、放送セル復号部１０２に供給された受信セルは、暗号鍵抽出部１０５の抽出出力を使って復号される。この復号出力は、セレクタ１０４に供給される。

【００７３】セル判定部１０３に供給された受信セルは、通常セル（暗号鍵セルを含む）か放送セルかを判定される。この判定結果は、セレクタ１０４に供給される。セレクタ１０４は、受信セルが通常セルの場合は、通常セル復号部１０１の復号出力を選択し、放送セルの場合は、放送セル復号部１０２の出力を選択する。

【００７４】これにより、受信セルが通常セルの場合は、通常セル復号部１０１の復号出力が暗号鍵抽出部１０５と、データ抽出部１０６に供給される。これに対

し、放送セルの場合は、放送セル復号部１０２の復号出力がこれらに供給される。

【００７５】暗号鍵抽出部１０５は、セレクタ１０４の選択出力から暗号鍵Ｋ２を抽出する。この抽出出力は、放送セル復号部１０２に復号用の暗号鍵として供給される。データ抽出部１０６は、セレクタ１０４の選択出力からペイロードに挿入されているデータを抽出する。但し、この抽出は、入力セルが暗号鍵セルである場合は、中止される。抽出されたデータは、データ復号部１０７によりディジタル信号からアナログ信号に戻される。

【００７６】通常セルの暗号化に用いられた暗号鍵Ｋ１が自端末に付与された暗号鍵Ｋ１と一致する場合、この通常セルは正確に復号される。これにより、この場合は、この通常セルのペイロードに挿入されているデータが正確に抽出される。その結果、この場合は、この通常セルを使って送られてきた情報が正確に再生されることになる。

【００７７】また、この場合、この通常セルが暗号鍵セルであれば、この暗号鍵セルから暗号Ｋ２が正確に抽出される。これにより、この場合は、放送セルが正確に復号される。その結果、この場合は、この放送セルのペイロードに挿入されているデータが正確に抽出される。これにより、この場合は、この放送セルを使って送られてきた情報が正確に再生されることになる。

【００７８】これに対し、通常セルの暗号化に用いられた暗号鍵Ｋ１が自端末に付与された暗号鍵Ｋ１と一致しない場合は、この通常セルが正確に復号されない。これにより、この場合は、この通常セルを使って送られてきた情報が正確に再生されないことになる。

【００７９】また、この場合は、暗号鍵Ｋ２も正確に抽出されないので、放送セルも正確に復号されない。これにより、この場合は、この放送セルを使って送られてきた情報が正確に再生されないことになる。

【００８０】以上詳述したこの実施例によれば、次のような効果が得られる。

【００８１】（１）　まず、この実施例によれば、放送セルを所定の周期で更新される暗号鍵Ｋ２を使って暗号化して送信し、かつ、この暗号鍵Ｋ２が更新されるたびに、この暗号鍵Ｋ２をセル化し、かつ、この暗号鍵セルを各契約者ごとに予め付与された暗号鍵Ｋ１を使って暗号化して送信するようにしたので、各加入者線９０に複数の契約端末１００が接続されている場合であっても、これらに一度で放送セルを放送することができる。

【００８２】これにより、時間的な放送スイッチを用いることなく、各加入者線９０に接続された複数の契約端末１００に放送セルを供給することができるので、各加入者の使用帯域が狭められるという問題と、バッファメモリの負荷や量が大きくなるという問題を回避することができる。

【００８３】（２）　また、この実施例によれば、暗号鍵Ｋ２を所定の周期で更新するようにしたので、契約が番組単位で更新されるような契約においては、暗号鍵Ｋ２の更新周期を例えば５分単位とすることにより、この暗号鍵Ｋ２の更新によって、実質的に契約を解除することができるという利点が得られる。一方、契約が年単位で更新されるような契約においては、暗号鍵Ｋ２の更新によって、この暗号鍵Ｋ２の秘密性を高めることができるという利点が得られる。

【００８４】（３）　また、この実施例によれば、暗号鍵Ｋ２を契約者に送信する場合、予めすべての暗号鍵Ｋ２を送信するのではなく、この暗号鍵Ｋ２が更新されるたびに、１つづつ送るようにしたので、暗号鍵Ｋ２として、乱数を用いることができる。これにより、暗号鍵Ｋ２の秘密性を高めることができる。

【００８５】（４）　さらに、この実施例によれば、暗号鍵Ｋ２を契約者に送信する場合、この暗号鍵Ｋ２をセル化した後、各契約者に付与された暗号鍵Ｋ１で暗号化して送信するようにしたので、この暗号鍵Ｋ２を通常セルの送信系を使って送信することができる。これにより、暗号鍵Ｋ２を送信するために追加するハードウェア量を極力少なくすることができる。

【００８６】以上、この発明の一実施例を説明したが、この発明は、上述したような実施例に限定されるものではない。

【００８７】（１）　例えば、先の実施例では、この発明を、パッシブダブルスター方式の加入者線９０を使った放送システムに適用する場合を説明した。しかし、この発明は、アクティブダブルスター方式の加入者線を使った放送システムに適用しても構わない。すなわち、契約者を含む複数の加入者に放送を行うシステムだけでなく、契約者のみに放送を行うシステムに適用しても構わない。

【００８８】（２）　また、先の実施例では、この発明を、セル交換方式のような蓄積交換方式の通信網を使って放送を行う放送シテムに適用する場合を説明した。しかし、この発明は、回線交換方式の通信網を使って放送を行う放送システムにも適用することができる。

【００８９】（３）　また、先の実施例では、この発明を、交換方式の通信網を使って放送を行う放送システムに適用する場合を説明した。しかし、この発明は、交換方式の通信網ではなく、例えば、複数のノードがメッシュ状に接続された通信網を使った放送システムにも適用することができる。

【００９０】（４）　このほかにも、この発明は、その要旨を逸脱しない範囲で、種々様々変形実施可能なことは勿論である。

【００９１】

【発明の効果】以上詳述したようにこの発明によれば、放送情報の送信信号を所定の周期で更新される第１の暗号鍵を使って暗号化して送信し、かつ、この暗号鍵が更

新されるたびに、この暗号鍵の送信信号を各契約者ごとに予め付与された第２の暗号鍵を使って暗号化して送信するようにしたので、１つの加入者線に複数の契約端末が接続されている場合であっても、これらに一度で放送情報を放送することができる。

【００９２】これにより、時間的な放送スイッチを用いることなく、各加入者線に接続された複数の契約端末に放送情報を供給することができるので、各加入者の使用帯域が狭められるという問題と、バッファメモリの負荷や量が大きくなるという問題を回避することができる。

【図面の簡単な説明】

【図１】この発明の一実施例の構成を示すブロック図である。

【図２】ＣＡＴＶシステムの一例の構成を示すブロック図である。

【図３】空間的放送スイッチの機能を説明するためのブロック図である。

【図４】時間的放送スイッチの機能を説明するためのブロック図である。

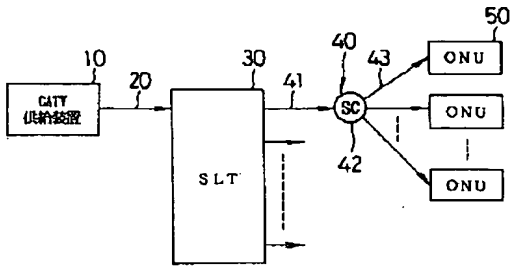
【図５】時間的放送スイッチの構成の一例を示すブロック図である。

【図６】時間的放送スイッチの構成の他の例を示すブロック図である。

【符号の説明】

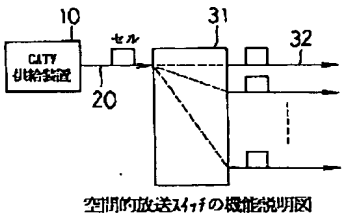
６０…ＣＡＴＶ供給装置
７０…長距離網
８０…加入者線終端装置
９０…加入者線
１００…加入者端末
８１…放送スイッチ
８２…加入者線インタフェース
９１，９３…光ファイバ
９２…スターカプラ
８２１…通常セル暗号化部
８２２…暗号鍵格納メモリ
８２３…放送セル暗号化部
８２４…暗号鍵発生部
８２５…時計部
８２６，１０３…セル判定部
８２７，８２８，１０４…セレクタ
８２９…セル化部
８３０…ファイル記憶部
１０１…通常セル復号部
１０２…放送セル復号部
１０５…暗号鍵抽出部
１０６…データ抽出部
１０７…データ復号部

【図２】



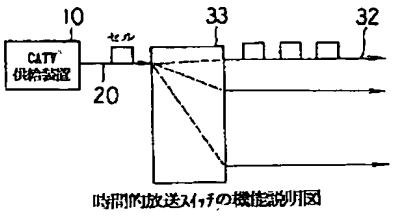
CATVシステムの構成図

【図３】



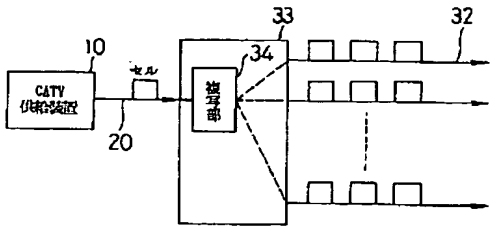
空間的放送スイッチの機能説明図

【図４】



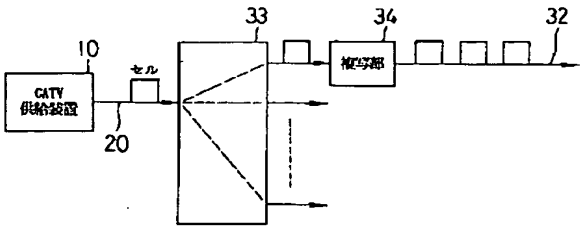
時間的放送スイッチの機能説明図

【図５】



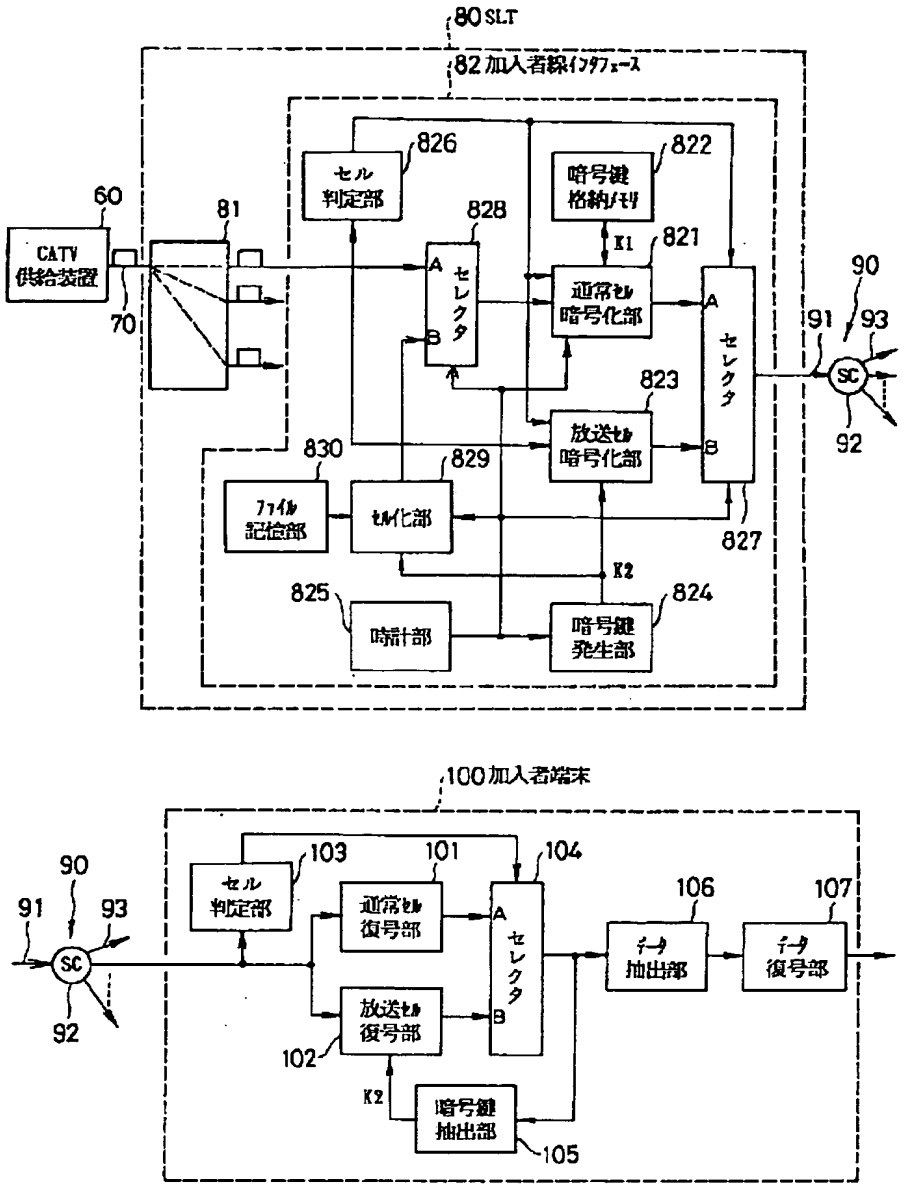
時間的放送スイッチの構成図

【図６】



時間的放送スイッチの構成図

【図１】



一実施例の構成図

フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	F I	技術表示箇所
H04N 7/167				